Styrelserna för Sjukhusen i väster, Sahlgrenska Universitetssjukhuset
och Fastighet, stöd och service
2025-12-10

Granskning av informationssäkerhet (REV 2025–00131)

Revisionen har granskat informationssäkerhet. Granskningen omfattar Sjukhusen i väster, Sahlgrenska Universitetssjukhuset och Fastighet, stöd och service. Syftet med granskningen var att bedöma om det bedrivs ett ändamålsenligt arbete med informationssäkerhet.

Vår bedömning är att Sjukhusen i västers arbete med informationssäkerhet i allt väsentligt är ändamålsenligt. Vidare är vår bedömning att Sahlgrenska Universitetssjukhuset samt Fastighet, stöd och service endast delvis har ett ändamålsenligt arbete. Vi lämnar fem rekommendationer till Sjukhusen i väster och åtta rekommendationer till Sahlgrenska Universitetssjukhuset samt Fastighet, stöd och service. På nästa sida finns de rekommendationer som vi lämnar med anledning av granskningen.

Vi önskar få ett yttrande från er senast den 26 juni 2026. Det ska framgå av yttrandet vilka åtgärder som ni har gjort eller planerar att göra med anledning av de rekommendationer som vi lämnar. Yttrandet skickar ni till revision@vgregion.se.

Revisionsrapporten översänds för yttrande till styrelserna för Sjukhusen i väster, Sahlgrenska Universitetssjukhuset och Fastighet, stöd och service samt för kännedom till regionfullmäktiges presidium och regionstyrelsen.

Vänersborg den 10 december 2025

För revisorskollegiet,

Krister Stensson,
ordförande

Vivi-Ann Nilsson,
vice ordförande

Rekommendationer

Revisionen rekommenderar styrelserna för Sahlgrenska Universitetssjukhuset, Sjukhusen i väster samt Fastighet stöd och service följande:

- Säkerställa fortsatt implementering av beslutade styrdokument som ingår i ledningssystem för informationssäkerhet och dataskydd (LISD).

- Påtala behov av att rutin för hantering av informationssäkerhetsincident upprättas och etableras i LISD till ansvariga.

- Säkerställa att organisationen är anpassad genom resurser och kompetens så att informationssäkerhetsarbetet har förutsättningar att vara systematiskt i enlighet med krav som ställs genom interna styrdokument och lagkrav.

- Vidta åtgärder för att höja deltagarantalet i grundutbildningar i syfte att säkerställa ett regelbundet genomförande.

- Säkerställa att uppföljning och rapportering av informationssäkerhets- och personuppgiftsincidenter sker med regelbundenhet.

Utöver det rekommenderar vi styrelserna för Sahlgrenska Universitetssjukhuset och Fastighet, stöd och service följande:

- Säkerställa att ansvar för styrelsen och förvaltningschefen upprätthålls i enlighet med dokumenterad ansvarsfördelning i interna styrdokument.

- Säkerställa att utbildning och informationsinsatser genomförs med högre grad av systematik så att insatser bidrar till en god säkerhetskultur inom informationssäkerhet.

- Säkerställa att ett uppföljningsarbete etableras som kan utgöra underlag till styrelsen i beslut om åtgärder för att stärka informationssäkerheten.

Granskning av informationssäkerhet

Rapport

Västra Götalandsregionen

2025-12-10

Antal sidor 26

Antal bilagor 3

1 INNEHÅLLSFÖRTECKNING

1 SAMMANFATTNING

Azets Revision & Rådgivning har av Västra Götalandsregionens förtroendevalda revisorer fått i uppdrag att granska om informationssäkerhetsarbetet hos styrelsen för Sahlgrenska universitetssjukhuset, styrelsen för Sjukhusen i väster samt styrelsen för Fastighet, stöd och service är ändamålsenligt.

Vår samlade bedömning utifrån granskningens syfte är att arbetet hos Styrelsen för sjukhusen i väster i allt väsentligt är ändamålsenligt.

Vår samlade bedömning utifrån granskningens syfte är att arbetet hos Styrelsen för Sahlgrenska universitetssjukhuset och Styrelsen för Fastighet, stöd och service endast delvis är ändamålsenligt.

Granskningen visar att det finns en tydlig styrning av informationssäkerhetsarbetet genom ledningssystem för informationssäkerhet och dataskydd (LISD). Styrelserna har god kännedom om regelverk och har kompletterat med lokal styrning utifrån behov inom respektive styrelse. Implementering av styrningen pågår inom utförarstyrelsernas verksamheter.

Vi bedömer att den ansvarsfördelning som regleras i riktlinjer för informationssäkerhet och dataskydd inte fullt ut följs. Vi ser risk att styrelsen för Sahlgrenska universitetssjukhuset, styrelsen för Fastighet, stöd och service samt förvaltningschefer inom dessa inte efterlever ansvarsfördelningen då vi inte har kunnat verifiera deras delaktighet i styrningen. Vi har kunnat verifiera att styrelsen och förvaltningschef hos Sjukhusen i väster deltar mer aktivt i både styrning och uppföljning. Vi bedömer därtill att det finns risk för att förvaltningschefer inte säkerställt informationssäkerhetsorganisationer med tillräckliga resurser och kompetens för att arbetet ska uppnå att vara systematiskt i enlighet med ansvar och krav som interna styrdokument anger.

Vår substansgranskning bekräftar god följsamhet till styrande dokument inom för arbetet med informationsklassning, riskhantering och kontinuitetshantering. Vi har noterat vissa förbättringsområden. Det saknas i regionens LISD dokumenterad rutin för hantering av informationssäkerhetsincidenter. Vi konstaterar dock att det i praktiken finns väl etablerad och känd process som används inom hela VGR. Rapportering av incidenter ska, enligt riktlinjerna, göras till styrelserna, vilket saknas i nuläget.

Ingen av styrelserna har säkerställt ett tillfredsställande genomförande av utbildningsinsatser vilket kan medföra risk för att medarbetare inte agerar tillräckligt säkert. Styrelsen för sjukhusen i väster har ett mer systematiskt arbete med utbildning riktat till olika funktioner och målgrupper, vilket saknas hos styrelsen för Sahlgrenska universitetssjukhuset och styrelsen för Fastighet, stöd och service.

Rutiner för uppföljning finns hos styrelsen för Sjukhusen i väster men saknas hos styrelsen för Sahlgrenska universitetssjukhuset och styrelsen för Fastighet, stöd och service.

I det följande redovisas samlad bedömning av revisionsfrågan per revisionsobjekt.

Finns en tillräcklig styrning av informationssäkerhetsarbetet?	
Styrelsen för Sjukhusen i väster	Endast delvis
Styrelsen för Sahlgrenska Universitetssjukhuset	Endast delvis
Styrelsen för Fastighet, stöd och service	Endast delvis
Arbetar styrelsen i enlighet med gällande regelverk inom informationssäkerhetsområdet?	
Styrelsen för Sjukhusen i väster	I allt väsentligt
Styrelsen för Sahlgrenska Universitetssjukhuset	I allt väsentligt
Styrelsen för Fastighet, stöd och service	I allt väsentligt
Sker en tillräcklig uppföljning av informationssäkerhetsarbetet?	
Styrelsen för Sjukhusen i väster	I allt väsentligt
Styrelsen för Sahlgrenska Universitetssjukhuset	Nej
Styrelsen för Fastighet, stöd och service	Nej

För närmare beskrivning av bakgrunden till våra bedömningar hänvisar vi till respektive avsnitt i revisionsrapporten.

Utifrån våra iakttagelser och bedömningar rekommenderar vi styrelsen för Sahlgrenska universitetssjukhuset, styrelsen för Sjukhusen i väster samt styrelsen för Fastighet, stöd och service att:

- Säkerställ fortsatt implementering av beslutade styrdokument som ingår i LISD
- Påtala behov av att rutin för hantering av informationssäkerhetsincident, upprättas och etableras i ledningssystem för informationssäkerhet och dataskydd till ansvariga.
- Säkerställ att organisationen är anpassad genom resurser och kompetens så att informationssäkerhetsarbetet har förutsättningar att vara systematiskt i enlighet med krav som ställs genom interna styrdokument och lagkrav.
- Vidta åtgärder för att höja deltagarantalet i grundutbildningar i syfte att säkerställa ett regelbundet genomförande.
- Säkerställa att uppföljning och rapportering av informationssäkerhets- och personuppgiftsincidenter sker med regelbundenhet.

Utöver det rekommenderar vi styrelsen för Sahlgrenska universitetssjukhuset och styrelsen för Fastighet, stöd och service att:

- Säkerställ att ansvar för styrelsen och förvaltningschef upprätthålls i enlighet med dokumenterad ansvarsfördelning i interna styrdokument.
- Säkerställa att utbildning och informationsinsatser genomförs med högre grad av systematik så att insatser bidrar till en god säkerhetskultur inom informationssäkerhet.
- Säkerställa att ett uppföljningsarbete etableras som kan utgöra underlag för styrelsen i beslut om åtgärder för att stärka informationssäkerheten.

2 BAKGRUND

Västra Götalandsregionen hanterar stora mängder känslig och skyddsvärd[1] information. Nämnder och styrelser ansvarar för att informationen behandlas och skyddas på ett ändamålsenligt sätt, samtidigt som tillgång och öppenhet säkerställs enligt offentlighetsprincipen.

Det övergripande målet för informationssäkerhet och skyddet för den personliga integriteten är att rätt och riktig information ska nå rätt mottagare i rätt tid och vara skyddad från obehörig åtkomst och förstörelse samt att samhällsviktig verksamhet kan upprätthållas på ett säkert och robust sätt. Därför är det viktigt att skydda informationen så att:

- den alltid finns när den behövs (tillgänglighet)
- den är tillförlitlig och korrekt och inte manipulerad eller förstörd (riktighet)
- endast tillgänglig för behöriga personer (konfidentialitet).

Informationssäkerhet är en fråga som inte bara berör verksamhetens ledning och säkerhetspersonal. Samtliga anställda i en verksamhet har ett ansvar för att uppnå och behålla en god informationssäkerhet. Det är därför viktigt att fördela och tydliggöra ansvar och roller i verksamheten samt att utbilda anställda i förhållande till arbetsuppgifter och ansvar[2].

Revisorskollegiet har pekat ut informationssäkerhet som ett viktigt område att granska i revisionsplanen för 2025. Om det finns brister i hur information hanteras kan det få allvarliga konsekvenser. Till exempel kan känslig information läcka ut eller det kan uppstå störningar i viktig samhällsverksamhet. Allvarliga och upprepade störningar kan leda till förtroendekriser, som också riskerar att sprida sig till fler aktörer och tjänster och även till andra sektorer.

Det är därför väsentligt att nämnder och styrelser har en tillräcklig intern styrning och kontroll av sitt informationssäkerhetsarbete så att arbetet sker på ett ändamålsenligt sätt.

Mot denna bakgrund har Västra Götalandsregionens revisorer beslutat att genomföra en granskning av regionens arbete med informations- och cybersäkerhet.

[1] Skyddsvärd innebär att informationen är värd att skydda med hänsyn till vad konsekvensen av skadan blir om tillgänglighet, riktighet och konfidentialitet röjs.
[2] Myndigheten för samhällsskydd och beredskap (2015). *En bild av kommunernas informationssäkerhetsarbete 2015* samt Riksrevisionen (2016). *Informationssäkerhetsarbete på nio myndigheter. En andra granskning av informationssäkerheten i staten*. RIR 2016:8.

3 SYFTE, REVISIONSFRÅGOR OCH AVGRÄNSNING

Granskningen har syftat till att bedöma om det bedrivs ett ändamålsenligt[3] arbete med informationssäkerhet.

Granskningen har besvarat följande revisionsfrågor:

- Finns en tillräcklig styrning av informationssäkerhetsarbetet?
- Arbetar styrelsen i enlighet med gällande regelverk inom informationssäkerhetsområdet?
- Sker en tillräcklig uppföljning av informationssäkerhetsarbetet?

3.1 AVGRÄNSNING

Granskningen har avgränsats till att omfatta Sahlgrenska Universitetssjukhuset, Sjukhusen i väster och Styrelsen för fastighet, stöd och service.

Granskningen avgränsas till styrning och ledning av informationssäkerhetsarbetet.

Granskningen omfattar inte informationssäkerhetsarbetet som rör tekniskt skydd och fysiskt skydd. I granskningen ingår inte heller att kontrollera och bedöma specifika IT-system eller applikationer.

Då revisionskriteriet *Informationssäkerhet och dataskydd - Riktlinje informationssäkerhet och dataskydd* omfattar både informationssäkerhet och dataskydd kommer vissa delar av personuppgiftshantering att ingå i granskningen. Bedömning av dessa delar kommer dock inte att inkluderas i rapporten då Dataskyddsförordningen inte utgör ett revisionskriterium.

4 REVISIONSKRITERIER

I granskningen har revisionskriterierna utgjorts av:

- 6 kap. 6 § kommunallagen (2017:725)
- Policy för säkerhet och beredskap (RS10162-1596316381-348)
- Informationssäkerhet och dataskydd - Riktlinje informationssäkerhet och dataskydd 2023–2027 (RS 2023–02811)
- Reglemente för berörda styrelser
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (även benämnt i rapporten som NIS-direktiv)

[3] Med formuleringen ändamålsenligt avser vi om arbetet med informationssäkerhet följer de krav och mål som gäller enligt riktlinjer och föreskrifter inom informationssäkerhetsområdet samt om det finns en styrning och uppföljning mot dessa bestämmelser.

Inom ramen för ändamålsenligt informationssäkerhetsarbete har vi granskat om arbete sker systematiskt med informationsklassificering, riskanalyser, incidenthantering, kontinuitetsplanering samt uppföljning och kontroll.

5 METOD

Granskningen har genomförts genom:

- Dokumentstudier, se Bilaga 1.
- Intervjuer med urval av representanter för respektive revisionsobjekt, se Bilaga 2.
- Stickprovsvisa kontroller av underlag för informationsklassning och riskbedömning för urval av system inom respektive granskningsobjekt.

De bedömningar som avlämnas i granskningen har utgått ifrån följande bedömningsnivåer.

Rapporten är faktakontrollerad av intervjupersoner.

6 RESULTAT AV GRANSKNINGEN

6.1 STYRNING OCH ORGANISATION

6.1.1 Ledningssystem för informationssäkerhet

Policy för säkerhet och beredskap[4] antaget av regionfullmäktige är det övergripande styrdokumentet för Västra Götalandsregionens (VGR) arbete med säkerhet. Policyn omfattar värderingar och förhållningssätt samt vilka förmågor regionen ska ha för att erhålla en god säkerhet och beredskap.

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster ställer krav på att de organisationer som bedriver samhällsviktig verksamhet ska ha ett etablerat ledningssystem för informationssäkerhet.

Regionstyrelsen har antagit dokumentet Informationssäkerhet och dataskydd – Regional riktlinje 2023–2027[5]. Enligt underlaget ingår riktlinjen i regionens ledningssystem för informationssäkerhet och dataskydd (LISD) vilket är styrande för alla förvaltningar och majoritetsägda bolag i VGR.

Riktlinjen beskriver hur LISD är uppbyggt och att det är inkluderat i Västra Götalandsregionens övergripande ledningssystem. LISD inkluderar mål, styrdokument, organisation och processer för informationssäkerhet, dataskydd, cybersäkerhet och it-säkerhet. Riktlinjen är baserad på standardserien SS-ISO/IEC 27000 för informationssäkerhet. Då interna styrdokument i VGR är anpassade efter de krav som ställs i lag om informationssäkerhet för samhällsviktiga och digitala tjänster, har vi bedömt att hänvisning till lagstiftning i rapporten endast görs i de fall där avvikelser identifieras.

Utöver riktlinjen finns tillhörande rutiner och stödjande material inom informationssäkerhet, dataskydd, cybersäkerhet och it-säkerhet som beskriver hur arbetet inom området ska genomföras. Enligt riktlinjen finns kompletterande styrande och stödjande dokument i en särskild förteckning. Vi har i granskningen tagit del av förteckning som presenterar de hittills framtagna och beslutade rutiner och stödmaterial som ingår i LISD. Genom vår dokumentgranskning noterar vi att rutiner och material tar sin utgångspunkt i informationssäkerhetsstandarden ISO27002 med hänvisning till olika krav och säkerhetsnivåer. Enligt riktlinjen kan förvaltningscheferna besluta om kompletterande lokal styrning inom området vid behov.

Intervjuade från flera revisionsobjekt ger en samstämmig bild av att regionens ledningssystem för informationssäkerhet och dataskydd har utvecklats positivt de senaste åren. Det har skett en uppdatering av både övergripande riktlinjer och majoriteten av rutiner. De intervjuade beskriver att krav och förväntningar i informationssäkerhetsarbetet har tydliggjorts genom arbetet. Samtidigt lyfts en osäkerhet i när LISD kommer vara komplett och vad som återstår att besluta om för styrningen framåt. Bland annat lyfts att rutin för hantering av

[4] 2025-01-07, Regionfullmäktige
[5] 2024-08-06, Regionstyrelsen

informationssäkerhetsincidenter saknas. Intervjuade har inte fått någon information med vad som återstår för att komplettera nuvarande LISD.

Förändringsarbetet uppges ha satt fokus på informationssäkerhetsfrågorna, vilket inneburit ett större engagemang och förståelse för vikten av ett mer strukturerat arbete.

Andra iakttagelser från intervjuer är behov av att anpassa LISD för att i högre grad beakta perspektiv för Medicinsk Teknik (MT). Det pågår ett regionövergripande arbete för att granska rutiner där genomgången hittills har visat att LISD är alltför omoget för att beakta specifika aspekter inom MT.

Som nämnts ovan så regleras i LISD att förvaltningschef har rätt att fatta beslut om lokalt anpassade rutiner och instruktioner. Inom samtliga revisionsobjekt har lokala rutiner och anvisningar etablerats. Exempel på rutiner vi tagit del av är:

- Sahlgrenska universitetssjukhuset (SU) - behörighetshantering, hantering av driftstörningar för it-system, rutin för dataskyddsorganisationen.
- Sjukhusen i väster (SV) – rutiner för hantering av personuppgiftsincidenter, lokal riktlinje och rutin för loggkontroller rutin för it-larm och akut it-störning.
- Fastighet, stöd och service (FSS) – rutiner avseende ansvar för IS/IT system, Rutin för att hantera digital samarbetsyta för fastighetsövergripande information, Rutin för att hantera skyddsvärd information, Manual för hantering av tjänster och behörigheter.

6.1.2 Organisation

Riktlinje för informationssäkerhet beskriver mål med ansvar och roller på följande sätt: *”Organisationen ska ha ett riskmedvetande och informationssäkerhetsarbetet ska vara organiserat så att det finns ett tydligt ansvar och följer ordinarie beredning- och beslutsprocesser. För att uppnå och bibehålla en god informationssäkerhet inom regionen ska ansvar definieras och tilldelas. Ansvaret sträcker sig från den politiska ledningen, genom tjänstemannaledningen till interna och externa medarbetare.”*

Av reglementen för styrelserna för Sjukhusen i väster [6], Sahlgrenska Universitetssjukhuset[7] samt Fastighet, stöd och service[8] framgår att respektive styrelse är personuppgiftsansvarig för de register och personuppgiftsbehandlingar som sker inom dess verksamhet. Respektive styrelse ska även utse ett dataskyddsombud. Vidare ansvarar styrelserna för säkerhet och beredskap inom sina verksamhetsområden.

Riktlinjer för informationssäkerhet beskriver övergripande ansvar för regionfullmäktige, regionstyrelsen, regiondirektör och centrala funktioner. Det ansvar som anges i reglementen bekräftas i riktlinjer för informationssäkerhet och dataskydd. Där anges att varje styrelse, nämnd och bolag ansvarar för informationssäkerheten och personuppgiftsbehandlingen som sker i egen verksamhet. Personuppgifter eller annan skyddsvärd information ska behandlas och skyddas på ett ändamålsenligt sätt i enlighet med tillämpligt regelverk.

[6] 2024-02-27, Regionfullmäktige
[7] 2024-02-27 Regionfullmäktige
[8] 2024-02-27, Regionfullmäktige

Förvaltningschef ansvarar för tillämpning av ledningssystemet för informationssäkerhet och dataskydd i den egna förvaltningen. Förvaltningschefen ska leda och stödja verksamheten för ett verkningsfullt ledningssystem för informationssäkerhet och dataskydd. Det ingår därtill i ansvaret att tillse att det finns resurser och kompetens för att bedriva ett systematiskt informations- och dataskyddsarbete.

Det har inte varit möjligt, genom dokumentgranskning och våra intervjuer, att få en tydlig bild över styrelsen för SU och styrelsen för FSS:s involvering i informationssäkerhetsarbetet. Det har inte heller varit möjligt att få en tydlig bild över hur förvaltningscheferna inom SU och FSS:s utövar ledning och stöd för informationssäkerhetsarbetet. Genom dokumentgranskning kan vi få bekräftat att Styrelsen för Sjukhusen i väster är en del i styrningen, bland annat genom beslut av årlig handlingsplan för arbetet samt beslut om organisation för informationssäkerhet och dataskydd. Vi kan därtill genom underlag verifiera att en löpande uppföljning och rapportering sker till förvaltningschef och årligen till styrelsen, se även avsnitt 6.3.2.

Informationsägare är en roll som beskrivs i LISD. Ansvaret uppges följa det ordinarie verksamhetsansvaret, exempelvis för avdelningschefer eller processägare. Informationsägaren ansvarar för att säkerställa implementation och efterlevnad av säkerhetsåtgärder utifrån krav på skydd för informationstillgångarna.

Iakttagelser från intervjuer för samtliga revisionsobjekt är att det finns en viss otydlighet över vad som ingår i rollen informationsägare samt en osäkerhet om det ansvar som tillskrivs rollen i de styrande dokumenten är etablerat inom samtliga verksamheter. Det finns därtill en upplevelse från informationsägare att deras ansvar ställer krav på kunskap, tid och stor delaktighet i det operativa arbetet. Önskemål finns om att snarare utgöra beslutsfattare när processer och aktiviteter har genomförts än att medverka i arbetet på detaljnivå. Det uppges även finnas behov av ytterligare stöd i utförandet från centrala funktioner i förvaltningen eller från Avdelning för säkerhet och beredskap på koncernkontoret.

Ägare av IS/IT-tjänst ansvarar enligt riktlinjerna för att införa, förvalta, följa upp och utvärdera säkerhetsåtgärder i IS/IT-tjänsten så att adekvat skydd uppnås. Detta ägarskap delas mellan förvaltningarna och Koncernstab digitalisering (KSD), beroende på om system och tjänster nyttjas regionövergripande eller inom respektive förvaltning.

Riktlinjerna ställer krav på att varje förvaltning ska ha en utsedd informationssäkerhets-samordnare och dataskyddssamordnare. Informationssäkerhetssamordnaren ska utgöra ett stöd till verksamheten i informationssäkerhetsarbetet och dataskyddssamordnaren är ett stöd till verksamheten i dess dataskyddsarbete. Båda rollerna ska verka för en regiongemensam tillämpning av interna styrdokument och regelverk i den egna verksamheten.

Samtliga revisionsobjekt har, i enlighet med krav i riktlinjer för informationssäkerhet, utsett informationssäkerhetssamordnare och dataskyddssamordnare. Intervjuade upplever att den förändring med högre ställda krav inom informationssäkerhet utifrån lagstiftning och interna styrdokument inte har åtföljts av förändring av resurser för arbetet. Det finns därför enligt de intervjuade behov av ytterligare resurser för att kunna möta verksamhetens behov inom informationssäkerhetsarbetet.

Av revisionsobjekten är det endast styrelsen för Sjukhusen i väster som genom beslut tydliggjort en intern organisation för arbetet med informationssäkerhet och dataskydd.

Intervjuade lyfter att beskrivningar i LISD saknar tydlighet gällande gränsdragning mellan förvaltningarna och KSD, exempelvis mellan informationsägare och ägare för IS/IT-tjänst då rollerna endast beskrivs översiktligt i nuvarande styrdokument. Vi har i granskningen fått information om att regionstyrelsen fattat beslut om att den tidigare styr- och samverkansmodellen för IS/IT inte längre ska gälla. Vi har efterfrågat en beskrivning av nya arbetsformer och organisering men någon sådan känner kontaktpersoner i granskningen inte till att det finns. Rollerna systemägare och systemförvaltare är vanligt förekommande i förvaltningarna och är även funktioner som deltagit i intervjuer i granskningen, dessa roller beskrivs inte i LISD. Intervjuade uppger att det finns en otydlighet kring roller inom regionens systemförvaltningsarbete i relation till informationssäkerhetsorganisationen.

Uppfattningen är att dessa roller på olika sätt genomför operativt arbete inom informationssäkerhet. Inom de revisionsobjekt som ingått i granskningen uppfattar vi en god samverkan mellan roller. Bilden från intervjuer är att utsedda samordnare och systemförvaltare har stort ansvar för framdrift i arbetet och att aktiviteter med grund i interna regelverk genomförs.

6.1.3 Utbildning och kompetens

Enligt riktlinjerna är mål för personalrelaterad säkerhet att *”Informationssäkerhetsåtgärder ska vara en del av anställningsprocessen och stå i proportion till verksamhetens krav, klassning av information som den anställde ska ges behörighet till och de risker som kan förekomma”.*

Riktlinjerna reglerar att personal ska göras medvetna om sina skyldigheter vid hantering av VGR:s information samt om gällande regler för informationssäkerhet och sekretess. Anställda ska få utbildning i informationssäkerhet och dataskydd utifrån vad som är relevant för medarbetarens arbetsuppgifter. Lämplig kunskapsnivå ska bibehållas under medarbetarens hela anställnings- eller uppdragstid.

Vi informeras om att HR-direktören på VGR har beslutat att utbildningen ”Digital informationssäkerhetsutbildning för alla (DISA)” är obligatorisk för samtliga medarbetare. Det finns även ytterligare en utbildning som är regiongemensam som riktar sig till vårdpersonal, ”Informationssäkerhet för hälso- och sjukvård”.

Information och kunskapsdelning för utsedda informationssäkerhetssamordnare sker löpande genom ett gemensamt forum där CISO[9]/Informationssäkerhetschef och centrala funktioner från Avdelning säkerhet och beredskap inom koncernkontoret samt regionövergripande dataskyddsfunktioner kan nå ut med aktuell information och utbildningsinsatser.

6.1.3.1 Styrelsen för Sahlgrenska Universitetssjukhuset

Uppföljning av Sahlgrenska Universitetssjukhusets genomförande av de regiongemensamma utbildningarna visar att[10]:

- Utbildningen DISA har genomförts av 4 895 av totalt 18 044 medarbetare (27 %).
- Utbildning av informationssäkerhet med inriktning hälso- och sjukvård har genomförts av 7 120 av totalt 20 433 medarbetare (35 %).

[9] Chief Information Security Officer, CISO, är den som leder och samordnar informationssäkerhetsarbetet i en organisation.

[10] Orsak till att totala antalet skiljer sig åt har inte kunnat redogöras för av kontaktpersoner.

Intervjuade uppger att det inte har genomförts några förvaltningsspecifika utbildningar eller andra insatser inom informationssäkerhet utöver de regionövergripande utbildningarna. Chefer genomför en grundutbildning där vissa inslag om informationssäkerhet ingår. Inom Sahlgrenska Universitetssjukhuset har utbildningen genomförts av 146 av totalt 780 chefer (19 %).

För samordnare inom MT har utbildningar i riskanalys genomförts, dock förs ingen statistik på deltagandet.

6.1.3.2 Styrelsen för Sjukhusen i väster

Uppföljning av Sjukhusen i västers genomförande av de regiongemensamma utbildningarna visar att[11]:

- Utbildningen DISA har genomförts av 885 av 2 992 medarbetare (29,6 %).
- Utbildning informationssäkerhet med inriktning hälso- och sjukvård har genomförts av 1 279 av 3 380 medarbetare (37,8 %).

Sjukhusen i väster har en utbildningsplan för informationssäkerhet och dataskydd 2024[12]. Intervjuade anger att planen för 2024 fortsatt gäller under 2025. Planen omfattar riktade insatser till prioriterade målgrupper: chefer, medarbetare inom staberna samt myndighetens informationssäkerhetskontakter. Behov och önskemål om utbildningsinsatser identifieras enligt uppgift löpande i verksamheterna. Utbildningar hålls av informationssäkerhetssamordnaren på plats ute i verksamheterna, vilket möjliggör ett mer verksamhetsnära stöd. Exempelvis har utbildningsinsatser riktade till verksamhetsledningar genomförts under 2025 där informationssäkerhetssamordnare i samverkan med dataskyddsombud och arkivansvarig besökt ledningsgrupperna. Därutöver har informationsinsatser och utbildning genomförts för olika yrkesgrupper enskilt och på arbetsplatsträffar, enligt önskemål från verksamheten. Vi har genom dokumentgranskning verifierat innehåll i utbildningar[13] som genomförts och kan konstatera att utbildningarna har inriktats på att stärka medarbetares kunskap om informationshantering, informationssäkerhet och dataskydd.

I Plan för intern kontroll 2025 för Sjukhusen i väster[14] visar uppföljning av ”*Kontroll avseende hantering av patientinformation och sekretess*” att det finns ytterligare behov av utbildningsinsatser för att stärka informationssäkerheten. Behovet omfattar både grundläggande utbildningar och mer verksamhetsanpassade insatser inom områden som informationshantering, informationssäkerhet och dataskydd.

6.1.3.3 Styrelsen för fastighet, stöd och service

Uppföljning från september 2025 av Fastighet, stöd och service genomförande av den regiongemensamma utbildningen visar att:

- Utbildningen DISA genomförts av 1649 av totalt 2602 medarbetare (63 %).

[11] Orsak till att totala antalet skiljer sig åt har inte kunnat redogöras för av kontaktpersoner.
[12] 2024-02-19
[13] Informationssäkerhet och dataskydd 2025-05-06, Så hanterar du information på rätt sätt i offentlig verksamhet (del 1) Allmänna handlingar och deras hantering, Så hanterar du information på rätt sätt i offentlig verksamhet (del 2) Informationssäkerhet och dataskydd.
[14] 2024-10-30, Styrelsen för Sjukhusen i väster, Dnr SV 2024-01383,

Några förvaltningsspecifika utbildningsinsatser har inte genomförts. I samband med informationssäkerhetsmånaden har visst utbildningsmaterial publicerats på förvaltningens intranät. Materialet har främst bestått av enklare bildspel med grundläggande budskap, såsom vikten av att skydda lösenord och att låsa datorskärmen.

6.1.4 Bedömning

Vår bedömning är att styrelsen för Sjukhusen i väster, styrelsen för Sahlgrenska Universitetssjukhuset samt styrelsen för Fastighet, stöd och service **endast delvis** säkerställt en tillräcklig styrning av informationssäkerhetsarbetet.

Vi baserar vår bedömning på att styrning i form av regionövergripande riktlinjer och rutiner i allt väsentligt finns etablerade i Västra Götalandsregionens ledningssystem för informationssäkerhet och dataskydd. Det pågår ett arbete att komplettera med ytterligare rutiner och utförarstyrelserna har ett pågående arbete att etablera den nya styrningen i verksamheterna. Vi noterar att utförarstyrelsernas arbete delvis påverkas av en osäkerhet då det inte är tydliggjort vilka ytterligare rutiner som är att vänta som styrning av informationssäkerhets- och dataskyddsarbetet. Vi noterar bland annat att regionövergripande rutin för hantering av informationssäkerhetsincident saknas.

Samtliga förvaltningar har beslutat om lokala rutiner vilket är i enlighet med beslutade riktlinjer för informationssäkerhet. Det pågår ett arbete med att utvärdera den regionövergripande styrningen i relation till lokala behov för att bedöma om ytterligare styrning behövs som komplement till LISD.

Vad gäller organisation för informationssäkerhetsarbetet så bedömer vi att detta endast delvis har säkerställts inom styrelserna. Det finns risk att styrelsen för Sahlgrenska universitetssjukhuset, styrelsen för Fastighet, stöd och service samt förvaltningschefer inom dessa inte följer ansvarsfördelningen enligt interna styrdokument. Vi har inte kunnat verifiera deras delaktighet i styrningen, där vi bedömer att styrelsen och förvaltningschef hos Sjukhusen i väster deltar mer aktivt. Vi bedömer att det finns risk för att förvaltningschefer inte säkerställt informationssäkerhetsorganisationer med tillräckliga resurser och kompetens för att arbetet ska uppnå att vara systematiskt i enlighet med interna styrdokument och lagkrav.

Vi bedömer vidare att granskade styrelser inte i tillräcklig utsträckning säkerställt kunskap och medvetenhet om informationssäkerhet eftersom granskningen visar att deltagandet i de regiongemensamma utbildningarna inte är tillfredsställande. Trots att utbildningar är obligatoriska visar uppföljning att samtliga styrelser behöver vidta åtgärder i syfte att höja deltagarantalet och säkerställa att grundutbildningar genomförs regelbundet.

Styrelsen i Väster har på ett systematiskt sätt planerat och genomfört utbildningar riktade till olika målgrupper inom förvaltningen vilket saknas inom styrelsen för Sahlgrenska universitetssjukhuset samt styrelsen för Fastighet, stöd och service. Vi bedömer därigenom att de krav som regleras i riktlinjer för informationssäkerhet gällande personalsäkerhet inte efterlevs.

6.2 FÖLJSAMHET TILL REGIONENS STYRANDE DOKUMENT INOM INFORMATIONSSÄKERHET

Avgränsning i den här granskningen har varit att bedöma följsamhet till styrande dokument och lagkrav inom följande områden: krav på förteckning av informationstillgångar, informationsklassning, riskhantering, incidenthantering, kontinuitetshantering och hantering av behörigheter.

6.2.1 Revisionskriterier

I riktlinjer för informationssäkerhet och dataskydd anges enskilda mål för riskhantering, informationsklassning, behörighetshantering, incidenthantering samt kontinuitetshantering. Därutöver reglerar riktlinjen tillsammans med tillhörande rutiner de krav som finns om respektive område.

Riskhantering

Riktlinjer för informationssäkerhet och tillhörande rutin för riskhantering[15] reglerar att informationssäkerhetsrisker som kan påverka Västra Götalandsregionens informationstillgångar och de registrerades integritet ska identifieras, analyseras, behandlas och följas upp.

Informationsklassning

Riktlinjer för informationssäkerhet och tillhörande rutin för informationsklassning[16] reglerar att verksamhetens information värderas utifrån vilka konsekvenser ett otillräckligt skydd för informationens konfidentialitet, riktighet och tillgänglighet skulle kunna få. Klassningsresultatet utgör underlag för att välja ändamålsenliga säkerhetsåtgärder.

Behörighetshantering

Riktlinjer för informationssäkerhet och tillhörande rutin för åtkomst till information och relaterade tillgångar[17] reglerar att all åtkomst ska styras så att endast behöriga ska få tillgång till informationstillgångar. Informationsägaren ska besluta om tilldelning och avslut av behörigheter. Det är informationsägarens ansvar att användningen av behörigheter är säker inom verksamheten. Åtkomstkontroll omfattar en eller flera funktioner i ett system som syftar till att reglera och kontrollera användares åtkomst till information och resurser. Det kan exempelvis handla om administrativa funktioner som implementeras i processer eller tekniska funktioner som implementeras i programvara, applikation eller IS/IT-tjänster.

Incidenthantering

Av riktlinjerna framgår att VGR ska ha rutiner på plats för att kunna bedöma om en informationssäkerhetshändelse är en informationssäkerhetsincident eller personuppgiftsincident. Informationssäkerhetsincidenter ska rapporteras, dokumenteras, eskaleras och följas upp inom respektive styrelse, nämnd, bolag samt på regional nivå. Omfattande och allvarliga incidenter ska rapporteras till informationssäkerhetschefen och samordnas regionalt. Bevarande av bevis ska hanteras på ett verkningsfullt sätt, samt att lärdomar ska dras av inträffade incidenter för att stärka och förbättra säkerhetsåtgärderna. Uppföljning ska därefter ska inom den egna myndigheten.

[15] Godkänd av direktör (RS10162-1596316381-118)
[16] Godkänd av direktör (RS10162-1596316381-102)
[17] Godkänd av direktör (RS10162-1596316381-366)

Dokumenterad regionövergripande rutin för incidenthantering gällande informationssäkerhetsincidenter har inte presenterats i granskningen och saknas i den förteckning som vi tagit del av över innehåll i LISD. Det finns beslutad rutin för hantering av personuppgiftsincident. Företrädare från avdelning Säkerhet och beredskap på koncernkontoret har dock uppgett att rutinen ska revideras.

Kontinuitetshantering
Riktlinjer för informationssäkerhet samt tillhörande rutin för kontinuitetshantering av IS/IT-tjänst[18] reglerar krav för arbetet. Av rutinen framgår att det ska finnas kontinuitetshantering för att säkerställa tillgång till information, IS/IT-tjänster och funktioner som krävs för att upprätthålla av ledningen prioriterad verksamhet. Planeringen ska regelbundet testas och uppdateras.

Kontinuitetshantering av IS/IT-tjänst ska utgå från genomförd informationsklassning, främst avseende krav om tillgänglighet för de informationstillgångar som berörs. En del i bedömningen är att fastställa extra skyddsvärda informationstillgångar som stödjer de delar av verksamheten som anses samhällsviktiga eller verksamhetskritiska.

Ägare av IS/IT-tjänst ansvarar för att säkra kraven på kontinuitet i sin tjänst utifrån de krav som verksamheten har och ansvarar för att kontinuitetsplan för IS/IT-tjänsten tas fram. Planen omfattar åtgärder runt driftskontinuitet, redundans, backup och reservkapacitet som implementeras i syfte att minska störningar.

6.2.2 Övergripande iakttagelse avseende följsamhet till gällande regelverk

Som beskrivits tidigare i rapporten så har LISD reviderats och kompletterats under de senaste åren. Vissa rutiner uppges relativt nyligen publicerats vilket medför att informationssäkerhets-samordnarna i förvaltningarna ännu inte hunnit sätta sig in i alla regler. Det pågår ett arbete med att implementera styrningen i respektive förvaltning där olika processer kommit olika långt.

Substansgranskning
För att granska följsamhet till styrningen så har vi som metod i granskningen genomfört en substansgranskning. Denna har syftat till att verifiera följsamhet till interna styrdokument för arbetet med; Systemförteckning, informationsklassning, riskhantering samt kontinuitetshantering.

Metoden bestod av följande steg:

1. Systemförteckning efterfrågas som redovisar de system som förvaltningen är systemägare för. (i de fall systemägarskap saknas har ett urval gjorts av system som nyttjas i verksamheten och där förvaltningen utfört egna bedömningar och analyser).
2. Ett urval gjordes av två verksamhetsspecifika system per revisionsobjekt.
3. För dessa system gjordes en genomgång av dokumentation för att verifiera följsamhet till regionens styrande dokument som ingår i LISD.
4. Kompletterande intervjuer har genomförts med nyckelfunktioner med ansvar för systemen eller informationssäkerhetsarbetet. Exempelvis systemägare,

[18] Godkänd av direktör (RS10162-1596316381-279)

systemförvaltare, IS/IT-samordnare, informationsägare och informationssäkerhetssamordnare.

Granskning av följsamhet till regionens styrande dokument baseras på ovan avgränsning och är inte heltäckande för styrelsernas informationssäkerhetsarbete för samtliga informationstillgångar och system. Vissa iakttagelser från intervjuer, utöver det som framkommit i substansgranskningen, redovisas under respektive revisionsobjekt.

Bedömning av arbetet med behörighetshantering har inte baserats på substansgranskning. Detta då det urval av system som gjordes endast hade verifierat hanteringen inom styrelsen för Fastighet, stöd och service. Övriga system saknade krav om behörighetshantering då de tillhörde medicinsk teknik eller där systemägarskap och ansvar för behörighetshantering fanns inom KSD.

6.2.3 Följsamhet till riktlinjer och rutiner för informationsklassning och riskhantering

Sahlgrenska universitetssjukhuset, Sjukhusen i väster och Styrelsen för fastighet, stöd och service
Resultatet av substansgranskning för utvalda system (två per revisionsobjekt) bekräftar följsamhet till regionens riktlinjer och rutiner. Dokumentation har skett på avsedda mallar och är kompletta. Vi kan vidare konstatera att deltagare i genomförandet består av representanter från verksamheterna samt kompetenser inom IS/IT och samordnarroller. Informations-säkerhetssamordnaren har i samtliga fall utgjort metodledare för klassningsarbetet.

För identifierade risker har åtgärder föreslagits. Ansvariga för att vidta dessa har utsetts och vi har även genom dokumentationen kunnat verifiera att dessa etablerats och att risker därefter bedömts vara på en acceptabel nivå.

6.2.4 Övriga iakttagelser avseende informationsklassning och riskbedömning

Företrädare för samtliga revisionsobjekt beskriver i intervju att arbetet med informationsklassning och riskhantering sker i enlighet med gällande rutin i LISD när det kommer till nyanskaffning eller större förändringar av system. Inom SU är uppfattningen att rutinen efterlevs i hög grad men samtidigt beskrivs en osäkerhet avseende följsamhet då intervjupersoner i granskningen inte alltid deltar i genomförandet.

Om det finns risk för de registrerades integritet så finns i LISD krav om att en tröskelanalys ska genomföras. Även för detta finns en beslutad rutin[19] som förvaltningarna anger att de följer. Detta har inte ingått i substansgranskning att granska.

I större projekt genomförs enligt uppgift momenten på regional nivå genom att en processägare utses, vilket är i enlighet med interna regelverk. Representanter från verksamheterna beskriver vid intervju att de i dessa fall delges information om genomförda analyser. Intervjuade uppger att det finns en viss osäkerhet om dessa ska anses tillräckliga eller om det finns en förväntan att även förvaltningarna själva ska genomföra momenten enligt regionens rutiner.

Intervjuade beskriver samstämmigt att det finns informationstillgångar som hanteras i IS/IT-tjänster som varit i drift sedan länge där det med stor sannolikhet saknas informations-klassningar och riskanalyser. Underlag för riskhantering, informationsklassning och tröskelanalys

[19] Godkänd av direktör (RS10162-1596316381-258)

lagras inte på samlad yta inom förvaltningarna vilket innebär att det saknas uppfattning eller kännedom över i hur stor omfattning arbetet är genomfört.

6.2.5 Följsamhet till riktlinjer och rutiner för kontinuitetshantering för IS/IT-tjänst

Sahlgrenska universitetssjukhuset, Sjukhusen i väster och Styrelsen för fastighet, stöd och service
Samstämmiga uppgifter från intervjuade hos samtliga revisionsobjekt är att informationsklassning och tillhörande riskbedömning utgör grund för krav om kontinuitetshantering. För det urval av system som ingått i substansgranskningen har vi verifierat att underlag som beskriver kontinuitetsbehov finns.

Resultat av informationsklassningar har delgetts KSD som därefter tecknat avtal med förvaltningarna om de behov om kontinuitet som verksamheten bestämt. Detta regleras i så kallade SLA[20] som tecknas per system eller IT-tjänst. I SLA framgår krav om bland annat redundans, backup, säkerhetskopiering samt acceptabla avbrottstider osv. KSD ansvarar för att kontinuitetsplaner upprättas baserade på de krav som verksamheten ställt samt för att vidta it-säkerhetsåtgärder som resultatet visar behov om.

I intervjuer uppges att den samlade dokumentationen och de SLA som finns utgör grund för hur KSD i kritiska situationer med störningar eller avbrott har en tydlig bild och dokumentation över prioriteringsordning mellan regionens system. Detta då informationsklassningar och tillhörande analyser bedömt tillgänglighetskrav samt vilka system som nyttjas i samhällsviktig verksamhet eller är verksamhetskritiska.

Utöver det arbete som genomförs inom KSD i syfte att säkerställa tillgänglighet till IS/IT-tjänster har samtliga revisionsobjekt ett stort antal reservrutiner och instruktioner i händelse av att informationen inte är tillgänglig. Vi har i granskningen tagit del av närmare 30-tal rutiner från Sjukhusen i väster, där vissa är gemensamma för hela förvaltningen och vissa är specifika för respektive sjukhus. För Sahlgrenska Universitetssjukhuset har vi tagit del av tiotal rutiner som utgör exempel på de rutiner som finns. Inom Fastighet, stöd och service har vi fått muntliga uppgifter om att ett antal rutiner finns som nyttjas vid störningar och avbrott i de system som nyttjas inom förvaltningen. Vi har dock inte erhållit underlag som verifierar de muntliga uppgifterna.

6.2.6 Test av planer och rutiner

Enligt rutin för kontinuitetshantering av IS/IT-tjänst framgår att ägare av IS/IT-tjänst ansvarar för att det minst årligen utförs periodisk översyn och utvärdering av kontinuitetshanteringen av IS/IT-tjänst. Kontinuitetsplaner ska testas och övas regelbundet. Tester ska planeras med verksamheterna så att dessa inte påverkar de som använder IS/IT-tjänsten.

Intervjuade uppger att rutiner är välkända och att de nyttjas kontinuerligt vid både planerade och oplanerade störningar eller avbrott. Några planerade tester har dock inte genomförts som intervjuade från förvaltningarna känner till.

Styrelsen för Sjukhusen i väster har inom ramen för internkontroll 2025 kontroll av att det finns robusta rutiner för att hantera störningar och att patientuppgifter skyddas. Vi har i granskningen tagit del av uppföljning av internkontrollplan per april 2025. Uppföljning visar att rutiner testats

[20] Service Level Agreement.

vid ett större avbrott. Vid det tillfället fanns bra och tydliga rutiner där de kliniska verksamheterna hanterade avbrottet bra tack vare att de manuella rutinerna fanns tillgängliga. Som förslag på förbättringsområde identifierade mer regelbundna kontroller av länkar till manuella rutiner för att säkerställa att dessa är aktuella och leder till korrekt information.

6.2.7 Följsamhet till riktlinjer och rutiner för behörighetshantering

Då behörighetshantering sker som enskilda processer för respektive IS/IT-tjänst så har det inte varit möjligt att verifiera att behörighetshantering sker med följsamhet till regionens styrande dokument för vart och ett av dessa. Vår granskning har därför inriktats på att få en samlad bild över rutiner och kontroller på övergripande nivå.

Vad gäller åtkomsthantering och tilldelning av behörigheter så sker den på flera olika nivåer i VGR. Vi har i vår dokumentgranskning tagit del av både regionövergripande riktlinjer och rutiner men även lokalt upprättade rutiner för hur detta fungerar för enskilda system eller verksamheter.

Samstämmigt i intervjuer är att det för regiongemensamma system finns väl dokumenterade rutiner och även processer för beställning av behörigheter där även förändring och avslut av tilldelade behörigheter sker. Detta sker genom portal på intranätet. Det finns väl utvecklade beskrivningar med checklistor som stöd för behöriga beställare att utgå från i hanteringen. Tilldelning baseras på medarbetares roll, organisatoriska tillhörighet och tilldelade funktioner. Behörighetsmodeller finns inbyggt i systemen och tilldelning av grundbehörigheter sker med automatik som del i anställningsprocessen. Vissa kontroller vid beställningar görs av funktioner inom förvaltningarna, innan beställning läggs till KSD.

Sahlgrenska universitetssjukhuset

Sahlgrenska universitetssjukhuset har ett antal lokala rutiner inom behörighetshantering.[21] Inom SU används en behörighetsportal där beställningar av behörigheter registreras. Kopplat till processen finns en mall för risk- och behovsanalys som intervjuade uppger som välfungerande.

Intervjuade beskriver att kontroller av åtkomst främst sker genom loggranskning. Arbetet genomförs enligt rutin för loggranskning.[22] Syftet är att säkerställa att tillgången till journaluppgifter följer gällande lagar och regelverk. Informationssäkerhetssamordnaren får kännedom om genomförda loggkontroller på en övergripande nivå. Vi har i granskningen tagit del av exempel från genomförda kontroller. Uppföljning samt hantering av eventuella avvikelser sker hos berörd verksamhet. I ett av de exempel vi tagit del av fanns avvikelser som enligt dokumentationen överlämnats till verksamhetschef för vidare utredning.

Sjukhusen i väster

Av systemförteckningen som vi tagit del av framgår att SV inte är systemägare för något system. Riktlinjer och rutiner för åtkomsthantering tilldelar ägare av IS/IT-tjänst ansvaret för en korrekt åtkomsthantering.

Intervjuade beskriver att behörighetshantering inom förvaltning sker genom att anställande chef fyller i formulär för beställning med specificering av vilka behörigheter som efterfrågas. Formuläret skickas därefter till förvaltningens it-samordnare som kontrollerar beställningen. Vi

[21] Riktlinje för åtkomst till patientuppgifter samt Rutin för uppdragstilldelning av särskilda uppdrag.
[22] 2025-01-28, Sjukhusdirektör

informeras om att it-samordnaren vid behov ifrågasätter beställningen i de fall samordnaren upplever att förfrågan är avvikande i förhållande till ordinarie åtkomstrutiner.

Kontroll av åtkomst till information uppges främst utgöras av loggranskning, där Sjukhusen i väster har tagit fram lokala riktlinjer[23]. Av riktlinjerna framgår roller och ansvar, hur begäran av loggutdrag ska genomföras samt att dokumentation av loggranskningsprocessen sker i enlighet med informationshanteringsplanen. Därutöver har en särskild rutin för loggranskning i patientinformationssystem tagits fram[24]. Intervjupersoner uppger att arbetet med loggranskning sker utifrån riktlinjer och rutiner.

Fastighet, stöd och service
Inom Fastighet, stöd och service finns flertal riktlinjer och rutiner[25] för hantering av behörigheter.

För ett av de system som ingått i vår substansgranskning finns ett stort antal behörighetsmodeller som utgår från funktioner, roller och organisatorisk tillhörighet. Behov har identifierats avseende en mer restriktiv tilldelning av behörigheter i avsett system där åtgärder för detta pågår.

Enligt intervjuade fungerar behörighetshanteringen generellt väl. I syfte att kontrollera arbetet med behörighetshantering så ingår i styrelsens internkontrollplan 2025 kontroll av behörigheter i tre system. Uppföljning per april 2025, kontrollgenomgång 1[26] visar 45 avvikelser i ett av systemen, främst kopplat till bristande hantering vid avslut av anställning. För det andra systemet fanns inga avvikelser och för det tredje endast ett fåtal avvikelser.

Ett digitalt flöde har etablerats som åtgärd för att stärka behörighetshanteringen.

6.2.8 Följsamhet till riktlinjer och rutiner för incidenthantering
Som beskrivits inledningsvis i avsnitt för revisionskriterier saknas i LISD dokumenterad rutin för hantering av incidenter inom informationssäkerhet. Vi har tagit del av rutin för hantering av personuppgiftsincidenter och tillhörande rapportering.

Vi har däremot fått muntliga uppgifter med beskrivning av nuvarande arbetssätt för hantering av både informationssäkerhetsincidenter och personuppgiftsincidenter. Samstämmigt har framkommit att det finns ett gemensamt och väl etablerat arbetssätt inom VGR där rapportering sker i MedControl. Intervjupersoner uppger att alla avvikelser som anmäls via MedControl handläggs på samma sätt oavsett typ av avvikelse eller händelser[27]. Vi informeras att samtliga revisionsobjekt använder MedControl för hantering av avvikelser som inte är av akut eller mer allvarlig karaktär.

Vi har tagit del av en lathund för hur en avvikelse ska hanteras i MedControl. Enligt lathunden sker anmälan via systemet, där en kategorisering för vilken typ av avvikelse som skett görs, exempelvis informationssäkerhetsincident, personuppgiftsincident etc. I lathunden framgår att en händelsebeskrivning ska anges tillsammans med var händelsen upptäcktes. I formuläret ska

[23] Riktlinje för loggranskning, 2024-04-08, Ekonomichef
[24] Rutin för loggranskning i patientinformationssystem, 2024-04-08, Ekonomichef
[25] Rutin avseende ansvar för IS/IT system samt Manual för hantering av tjänster och behörigheter
[26] Datum och beslutsinstans saknas
[27] Arbetsskada, patientskada samt övrig avvikelse

anges om produkt, utrustning eller IT-system är inblandat. Samtliga avvikelser som anmäls via systemet dokumenteras i systemet och får då ett ärendenummer.

Intervjuade har förevisat inrapporterade incidenter där vi kan verifiera att dessa finns dokumenterade och kopplade till ett ärendenummer. Enligt intervjuade registreras sedan ytterligare dokumentation eller aktiviteter relaterade till incidenten med spårbarhet till ärendenumret.

Sahlgrenska universitetssjukhuset
Vi har i granskningen tagit del av säkerhetshandbok för Sahlgrenska universitetssjukhuset[28]. Av handboken framgår att incidentrapportering ska ske via MedControl. Anmälningar i MedControl når förvaltningens informationssäkerhetssamordnare, dataskyddssamordnare samt områdeskontakterna. Det är områdeskontakterna som gör bedömning avseende vilken typ av incident som har ägt rum. Eventuella åtgärder vidtas sedan inom den berörda verksamheten. Informationssäkerhetssamordnaren går ensam igenom samtliga incidenter i syfte att identifiera eventuella trender eller mönster.

Därutöver har SU vissa rutiner samt en handbok för avvikelser riktad till chefer. Rutin för driftstörningar i it-system samt it-larm[29] fungerar som en arbetsbeskrivning vid planerade och oplanerade stopp i driften. Rutinen innehåller information om vad som ska kontrolleras, vad anmälan ska innehålla samt vilka som är ansvariga och ska informeras.

Vi informeras om att det inte sker någon systematisk återrapportering av inträffade informationssäkerhetsincidenter till styrelsen, detta sker främst i samband med större incidenter.

Sjukhusen i väster
Samtliga anmälningar som görs avseende informationssäkerhet i avvikelsesystemet eskaleras till informationssäkerhetssamordnaren. Det är även denne som kategoriserar vilken typ av incident det är. Därefter utses roller som orsaksutredare och åtgärdsansvarig samt vem som ansvarar för att följa upp och avsluta ärendet. Vid återkommande händelser genomförs ett analysarbete internt på förvaltningen och vid behov vidtas åtgärder.

Av förvaltningens årsrapport för informationssäkerhet och dataskydd år 2024 framgår att styrelsen får återrapportering angående personuppgiftsincidenter. Motsvarande rapportering för informationssäkerhetsincidenter saknas.

Styrelsen för fastighet, stöd och service
Anmälda informationssäkerhetsincidenter eskaleras till förvaltningens informations-säkerhetssamordnare. I samband med en anmäld händelse utses en orsaksutredare inom berörd verksamhet. Därutöver har informationssäkerhetssamordnaren i uppgift att analysera händelsen på ett mer övergripande plan utifrån exempelvis trender och mönster.

Intervjuade beskriver dock risk för bristande kunskap om vad som utgör en informationssäkerhetsincident. Det framkommer även att det kan saknas tillräcklig förståelse för

[28] Säkerhetshandbok, Senast reviderad 2025-08-18
[29] Beslutad av direktör, SU9771-677637494-133

hur en sådan incident ska anmälas. Mot denna bakgrund finns en risk att inträffade incidenter inte identifieras eller rapporteras.

Det saknas etablerade rutiner för återrapportering av inträffade incidenter till styrelsen. När återrapportering sker är det på förekommen anledning.

6.2.9 Bedömning

Vår bedömning är att styrelsen för Sahlgrenska Universitetssjukhuset, styrelsen för Sjukhusen i väster och styrelsen för Fastighet, stöd och service i allt väsentligt arbetar i enlighet med gällande regelverk inom informationssäkerhetsområdet.

Vi baserar vår bedömning på att styrelserna visar på god kännedom om de riktlinjer och rutiner som hittills styr regionens informationssäkerhetsarbete. Då styrningen beslutats under 2024 och framåt pågår arbete att implementera styrningen inom utförarstyrelsernas verksamheter.

Vår substansgranskning bekräftar i allt väsentligt följsamhet till riktlinjer och rutiner för samtliga styrelser gällande arbetet med informationsklassning, riskhantering samt kontinuitetshantering, för de system som ingår i urval för substansgranskningen.

I nuläget saknas beslutad rutin för hantering av informationssäkerhetsincidenter vilket regionens riktlinjer för informationssäkerhet uttrycker ska finnas. Rutin för hantering av personuppgiftsincidenter finns beslutad. Vi uppfattar dock att lathund för registrering av avvikelser utgör grund för hantering av informationssäkerhetsincidenter vilken samtliga förvaltningar arbetar utifrån. Vi bedömer att arbetssättet är välfungerande och innebär att det finns en samlad och strukturerad dokumentation för inträffade incidenter. Vi bedömer dock att arbetssättet bör dokumenteras i en rutin samt att incidenter rapporteras till styrelserna i enlighet med krav i riktlinjerna.

Då samtliga styrelsers tilldelning, avslut samt ändring av behörigheter i hög grad baseras på manuell hantering så bedömer vi att det finns behov av att tydliggöra krav på uppföljning och kontroll av behörigheter. Detta för att säkerställa att endast behöriga har åtkomst till information i enlighet med krav i riktlinjer, rutiner och lagkrav. Vi ser positivt på att kontroller av behörigheter inkluderats i internkontroll hos Fastighet, stöd och service samt genom regelbunden loggkontroll enligt gällande rutiner inom Sahlgrenska universitetssjukhuset och Sjukhusen i väster. Vi kan dock inte utesluta att nuvarande kontroller inte i tillräcklig grad identifierar risker och brister då urvalet endast är av karaktären stickprov med relativt litet urval.

7 UPPFÖLJNING

Mål enligt riktlinje för informationssäkerhet och dataskydd är att *"Informationssäkerheten och informationssäkerhetsarbetet ska, som en del av den ordinarie verksamhetsredovisningen, regelbundet följas upp på central nivå och inom respektive nämnd, styrelse och bolag".*

Krav på uppföljning anges i riktlinjer för informationssäkerhet och dataskydd där ansvaret för detta ser ut som följer:

- Styrelsen har i ansvar att kontinuerligt följa upp verksamheten och säkerställa att den får tillräcklig information.
- Förvaltningschef ansvarar för att rapportera till den egna styrelsen med hjälp av informationssäkerhetssamordnare och dataskyddsamordnare.
- Samordnarna följer upp den egna förvaltningens informationssäkerhets- och dataskyddsarbete, på eget initiativ efter verksamhetens behov samt som ett led i regional uppföljning.

De metoder som anges som möjliga är genom internkontroll eller årlig säkerhetsrapport.

Regional rutin för uppföljning och rapportering[30] är en rutin som är en del av regionens LISD. Rutinen anger att uppföljning sker genom övervakning, mätning, analys och utvärdering av områden som tillämpning, säkerhetsåtgärder, mognadsnivå, måluppfyllnad och riskbild.

Rapportering ska utöver vad som anges ovan även ske löpande till informationssäkerhetschef, årligen till säkerhets- och beredskapschef och vidare till högsta ledning som använder underlaget för beslut om förbättringar.

7.1.1 Styrelsen för Sahlgrenska Universitetssjukhuset

Enligt uppgift sker ingen samlad uppföljning av informationssäkerhetsarbetet inom Sahlgrenska Universitetssjukhuset.

I Plan för intern kontroll 2025 för Sahlgrenska Universitetssjukhuset[31] har området informationshantering och it identifierats som ett riskområde, baserat på genomförd riskvärdering. Den övergripande risken är *"Risk att SU inte är tillräckligt förberett*

vid införande av nytt vårdinformationssystem" där två kontroller ingår att följa upp under året:

1. Följa det regionala arbetet med extern granskning av införandet av Millennium
2. Följa upp förberedelsearbetet av nytt vårdinformationssystem.

Uppföljning av intern kontroll[32] visade att inga eller få avvikelser och har därigenom inte föranlett några behov av åtgärder.

7.1.2 Styrelsen för Sjukhusen i väster

Arbetet med informationssäkerhet inom Sjukhusen i väster sker utifrån en handlingsplan[33]. Syftet med handlingsplanen är att beskriva förvaltningens årliga informations- och

[30] 2024-12-20, Direktör
[31] 2024-12-13
[32] Styrelsen för SU - Uppföljning av plan för intern kontroll, kontroll per april 2025
[33] Beslutad av styrelsen 2024-02-28.

dataskyddsarbete. Handlingsplan för 2025 innehåller mål för styrelsens arbete och prioriterade aktiviteter som behöver genomföras i syfte att stärka arbetet. I uppföljning från tidigare års handlingsplaner noterar vi att styrelsen och även förvaltningschef tar del av regelbunden rapportering om framdriften i arbetet.

Inom Sjukhusen i väster sammanställs en årsrapport för informationssäkerhet och dataskydd som presenteras för styrelsen[34]. I rapporten redogörs för det arbete som skett under innevarande år utifrån fastställd handlingsplan.

I plan för intern kontroll 2025 för Sjukhusen i väster[35] har informationshantering och it identifierats som ett prioriterat riskområde, baserat på genomförd riskvärdering. Två kontroller ingår att följa upp under året:

1. Allvarlig it-störning
2. Att patientinformation hamnar fel

Uppföljning av intern kontroll[36] visade, som tidigare nämnts (se avsnitt 6.1.3.2), avvikelser angående hantering av patientinformation, där resultatet visar att det finns behov av insatser för att stärka kunskapen kring informationshantering. Resultat från kontroll avseende allvarlig it-störning visar att det finns bra och tydliga rutiner för hantering av it-avbrott.

7.1.3 Styrelsen för fastighet, stöd och service

Enligt uppgift sker ingen samlad uppföljning av informationssäkerhetsarbetet Inom Fastighet, stöd och service. Den uppföljning som finns är den som på övergripande nivå beskrivs i årsredovisningen.

I Plan för intern kontroll 2025 för Styrelsen för fastighet, stöd och service[37] har informationshantering och it identifierats som ett prioriterat riskområde, baserat på genomförd riskvärdering. Tre kontroller ingår att följa upp under året:

1. Behörighetshantering
2. Bemanning systemförvaltningsmodell
3. Överlämning av fastighetsinformation från projekt till förvaltning

Uppföljning av intern kontroll[38], visar som nämnts tidigare i rapporten, avvikelser gällande behörighetshantering för ett av de system som nyttjas inom förvaltningen. Övriga två system som kontrollerades hade inga eller få avvikelser. Kontroll av systemförvaltningsorganisation visade inga avvikelser. Dock hade kontrollen avseende överlämning av fastighetsinformation allvarlig avvikelse som krävde omedelbar åtgärd.

[34] Daterad 2024-12-12
[35] Datum och beslutsinstans saknas
[36] Styrelsen för SV - Uppföljning av plan för intern kontroll, kontroll per april 2025
[37] 2024-10-30, Styrelsen för Sjukhusen i väster, Dnr SV 2024-01383
[38] Styrelsen för FSS - Uppföljning av plan för intern kontroll, kontroll per april 2025

7.1.4 Bedömning

Vår bedömning är att styrelsen för Sjukhusen i väster **i allt väsentligt** har en tillräcklig uppföljning av informationssäkerhetsarbetet.

Vi baserar vår bedömning på att styrelsen för Sjukhusen i väster etablerat rutiner för årlig uppföljning av beslutad handlingsplan för förvaltningens arbete i enlighet med krav i riktlinjer för informationssäkerhet. Genom nuvarande uppföljning kan både mål och prioriterade aktiviteter följas av styrelsen i syfte att identifiera ytterligare förbättringsområden. Vi bedömer att nuvarande rapportering bör kompletteras med uppföljning av inträffade informationssäkerhetsincidenter. Det finns utöver ovan även kontroller inom ramen för styrelsens internkontroll 2025. Vi bedömer att dessa kompletterar övriga uppföljning utifrån bedömda risker för verksamheten.

Vår bedömning är att styrelsen för Sahlgrenska Universitetssjukhuset och styrelsen för Fastighet, stöd och service **inte** har en tillräcklig uppföljning av informationssäkerhetsarbetet.

Vi baserar vår bedömning på att det saknas dokumenterad uppföljning av informationssäkerhetsarbetet vilket är ett krav enligt riktlinjer för informationssäkerhet. Det saknas även regelbunden rapportering till styrelserna för att de ska ha insyn i det arbete som genomförs i syfte att ta ansvar för verksamheten. Vi bedömer därigenom att uppföljningen inte motsvarar kraven i interna regelverk. Styrelserna har inkluderat informationssäkerhetsområdet i sina internkontrollplaner 2025 vilket enligt riktlinjer för informationssäkerhet är ett möjligt alternativ för uppföljning. Vår bedömning är dock att nuvarande kontroller inte utgör en tillräcklig uppföljning av informationssäkerhetsarbetet på ett övergripande plan. Kontrollerna fångar väsentliga delar av informationssäkerhet men motsvarar i vår mening inte den uppföljning som ska ske enligt riktlinje för informationssäkerhet samt rutin för uppföljning och rapportering.

8 SAMLAD BEDÖMNING OCH REKOMMENDATIONER

Granskningen har syftat till att bedöma om det bedrivs ett ändamålsenligt arbete med informationssäkerhet.

Vår samlade bedömning utifrån granskningens syfte är att styrelsernas arbete endast delvis är ändamålsenligt.

Utifrån våra iakttagelser och bedömningar rekommenderar vi styrelsen för Sahlgrenska universitetssjukhuset, styrelsen för Sjukhusen i väster samt styrelsen för Fastighet, stöd och service att:

- Säkerställ fortsatt implementering av beslutade styrdokument som ingår i LISD
- Påtala behov av att rutin för hantering av informationssäkerhetsincident, upprättas och etableras i ledningssystem för informationssäkerhet och dataskydd till ansvariga.
- Säkerställ att organisationen är anpassad genom resurser och kompetens så att informationssäkerhetsarbetet har förutsättningar att vara systematiskt i enlighet med krav som ställs genom interna styrdokument och lagkrav.
- Vidta åtgärder för att höja deltagarantalet i grundutbildningar i syfte att säkerställa ett regelbundet genomförande.
- Säkerställa att uppföljning och rapportering av informationssäkerhets- och personuppgiftsincidenter sker med regelbundenhet.

Utöver det rekommenderar vi styrelsen för Sahlgrenska universitetssjukhuset och styrelsen för Fastighet, stöd och service att:

- Säkerställ att ansvar för styrelsen och förvaltningschef upprätthålls i enlighet med dokumenterad ansvarsfördelning i interna styrdokument.
- Säkerställa att utbildning och informationsinsatser genomförs med högre grad av systematik så att insatser bidrar till en god säkerhetskultur inom informationssäkerhet.
- Säkerställa att ett uppföljningsarbete etableras som kan utgöra underlag för styrelsen i beslut om åtgärder för att stärka informationssäkerheten.

Datum som ovan

Azets Revision & Rådgivning AB

Veronica Hedlund Lundgren
Certifierad kommunal revisor

Jenny Thörn
Verksamhetsrevisor

Ida Larsson
Verksamhetsrevisor

Hilda Vejdeland
Verksamhetsrevisor

BILAGA 1 STYRANDE DOKUMENT

Följande styrande och stödjande dokument har ingått i granskningen:

- Reglementen för styrelser och nämnder
- Policy för säkerhet och beredskap 2025–2029
- Riktlinje för informationssäkerhet och dataskydd 2023 – 2027
- Rutiner, mallar och instruktioner som ingår i VGR ledningssystem för informationssäkerhet och dataskydd (LISD).
- Riskanalysmall 2024
- GAP analysmall 2024 ISOIEC 27002_2022

Fastighet, stöd och service

- Ansvar avseende ISIT-system – Rutin
- Bedömning av skyddsvärden – Riktlinje
- Hantera digital samarbetsyta för tomtövergripande information, Rågården – Rutin
- Hantera skyddsvärd information, Rågården – Rutin
- Hantering av tjänster och behörigheter – Manual
- Plan för intern kontroll SFSS 2025
- Styrelsen för fastighet stöd och service – Reglemente
- Systemägare och systemförvaltare per verksamhetssystem – Förteckning
- Systemägare och systemförvaltare per verksamhetssystem – Utvalda
- Uppföljning plan för intern kontroll per april
- Årsredovisning 2024 Styrelsen för fastighet stöd och service

Sahlgrenska universitetssjukhuset

- Aktiv avvikelsehantering för en lärande organisation– Häfte
- Behovs- och riskanalys behörighet till journalsystem
- Dataskyddsorganisationen för Sahlgrenska
- Driftstörning – för respektive system Elvis, Medspeech, Melior
- Driftstörningar i it-system samt it-larm
- Informationsklassning CPMS 2.0
- Informationsklassning av Hjärt-lungmaskin thoraxkirurgi SU
- InterInfo – återrapportering av blodkomponenter
- Kontaktuppgifter och åtgärder vid problem i VNL
- Loggranskningsrutin
- Manuella rutiner vid driftstörning – driftstopp i e-arkiv
- Plan för intern kontroll 2025
- Reservrutin beställning av läkemedel från RGL
- Riskhantering - Hjärt-lungmaskin thoraxkirurgi SU
- Riskhantering för informationssäkerhet – CPMS 2.0

- Sekretess inom hälso- och sjukvården
- Statistik SU - informationssäkerhetsutbildningar
- Styrelsen för Sahlgrenska Universitetssjukhuset – Reglemente
- Uppdragstilldelning av särskilda uppdrag
- Uppföljning 1 av Plan för intern kontroll 2025
- Årsberättelse 2024
- Åtkomst till patientuppgifter

Sjukhusen i väster

- Beslut om informationssäkerhetsorganisation
- DISA – Genomförande till och med 15 oktober 2025
- Handlingsplan för informationssäkerhet- och dataskyddsarbetet för år 2025
- Informationsklassning SDK
- Informationssäkerhet och dataskydd 20250506
- Informationssäkerhet och dataskyddsarbete inom Sjukhusen i väster 2023
- Informationssäkerhet och dataskyddsarbete inom Sjukhusen i väster 2024
- Lathund dataskyddssamordnare
- Lathund medarbetare, chef och orsaksutredare
- Loggranskning i patientinformationssystem inom Sjukhusen i väster – Rutin
- Loggranskning inom Sjukhusen i väster – Riktlinje
- Loggranskning okt 24, 1
- Loggranskning okt 24, 2
- Loggranskning okt 24, 3
- Personuppgifter och incidenter okt 24 1
- Personuppgifter och incidenter okt 24 2
- Personuppgifter och incidenter okt 24 3
- Plan för intern kontroll 2025 för Sjukhusen i väster
- Presentation av årsrapport 2024
- Rapportering till förvaltningschef 240619
- Riskhantering för informationssäkerhet SDK
- Skärmbild infosäkmånaden 2025
- Styrelsen för Sjukhusen i väster, Reglemente
- Så hanterar du information på rätt sätt i offentlig verksamhet del 1
- Så hanterar du information på rätt sätt i offentlig verksamhet del 2
- System SV
- Tänk säkert 25
- Uppföljning av plan för intern kontroll 2025 för Sjukhusen i väster per april
- Uppföljning av plan för intern kontroll 2025 för Sjukhusen i väster per augusti
- Utbildningsplan för informationssäkerhet och dataskydd 2024
- Årsrapport informationssäkerhet 2024
- Överenskommelse 2025 SÄLMA Samarbete SU och SV

BILAGA 2 INTERVJUPERSONER

Fastighet, stöd och service

- Informationssäkerhetssamordnare
- IT-chef
- Systemägare och systemförvaltare system 1
- Systemförvaltare system 2

Sahlgrenska Universitetssjukhuset

- Informationssäkerhetsamordnare
- Dataskyddssamordnare
- Informationssäkerhetssamordnare MT
- Samordnare och projektledare inom medicinteknik och it system 3

Sjukhusen i väster

- Informationssäkerhetssamordnare
- Enhetschef kanslienheten
- Jurist
- Ansvarig för behörighetshantering inom IS, E-hälsa och IS/IT
- Biträdande utgivare av SITHS

BILAGA 3 REKOMMENDATIONER PER REVISIONSOBJEKT

REKOMMENDATIONER STYRELSEN FÖR SAHLGRENSKA UNIVERSITETSSJUKHUSET

Utifrån våra iakttagelser och bedömningar rekommenderar vi styrelsen för Sahlgrenska universitetssjukhuset att:

- Säkerställ fortsatt implementering av beslutade styrdokument som ingår i LISD
- Påtala behov av att rutin för hantering av informationssäkerhetsincident, upprättas och etableras i ledningssystem för informationssäkerhet och dataskydd till ansvariga.
- Säkerställ att organisationen är anpassad genom resurser och kompetens så att informationssäkerhetsarbetet har förutsättningar att vara systematiskt i enlighet med krav som ställs genom interna styrdokument och lagkrav.
- Vidta åtgärder för att höja deltagarantalet i grundutbildningar i syfte att säkerställa ett regelbundet genomförande.
- Säkerställa att uppföljning och rapportering av informationssäkerhets- och personuppgiftsincidenter sker med regelbundenhet.
- Säkerställ att ansvar för styrelsen och förvaltningschef upprätthålls i enlighet med dokumenterad ansvarsfördelning i interna styrdokument.
- Säkerställa att utbildning och informationsinsatser genomförs med högre grad av systematik så att insatser bidrar till en god säkerhetskultur inom informationssäkerhet.
- Säkerställa att ett uppföljningsarbete etableras som kan utgöra underlag för styrelsen i beslut om åtgärder för att stärka informationssäkerheten.

REKOMMENDATIONER STYRELSEN FÖR SJUKHUSEN I VÄSTER

Utifrån våra iakttagelser och bedömningar rekommenderar vi styrelsen för Sjukhusen i väster att:

- Säkerställ fortsatt implementering av beslutade styrdokument som ingår i LISD
- Påtala behov av att rutin för hantering av informationssäkerhetsincident, upprättas och etableras i ledningssystem för informationssäkerhet och dataskydd till ansvariga.
- Säkerställ att organisationen är anpassad genom resurser och kompetens så att informationssäkerhetsarbetet har förutsättningar att vara systematiskt i enlighet med krav som ställs genom interna styrdokument och lagkrav.
- Vidta åtgärder för att höja deltagarantalet i grundutbildningar i syfte att säkerställa ett regelbundet genomförande.
- Säkerställa att uppföljning och rapportering av informationssäkerhets- och personuppgiftsincidenter sker med regelbundenhet.

Rekommendationer Styrelsen för Fastighet, stöd och service

Utifrån våra iakttagelser och bedömningar rekommenderar vi styrelsen för Fastighet, stöd och service att:

- Säkerställ fortsatt implementering av beslutade styrdokument som ingår i LISD
- Påtala behov av att rutin för hantering av informationssäkerhetsincident, upprättas och etableras i ledningssystem för informationssäkerhet och dataskydd till ansvariga.
- Säkerställ att organisationen är anpassad genom resurser och kompetens så att informationssäkerhetsarbetet har förutsättningar att vara systematiskt i enlighet med krav som ställs genom interna styrdokument och lagkrav.
- Vidta åtgärder för att höja deltagarantalet i grundutbildningar i syfte att säkerställa ett regelbundet genomförande.
- Säkerställa att uppföljning och rapportering av informationssäkerhets- och personuppgiftsincidenter sker med regelbundenhet.
- Säkerställ att ansvar för styrelsen och förvaltningschef upprätthålls i enlighet med dokumenterad ansvarsfördelning i interna styrdokument.
- Säkerställa att utbildning och informationsinsatser genomförs med högre grad av systematik så att insatser bidrar till en god säkerhetskultur inom informationssäkerhet.
- Säkerställa att ett uppföljningsarbete etableras som kan utgöra underlag för styrelsen i beslut om åtgärder för att stärka informationssäkerheten.